Part I: Overview

Core concepts presented:

- What is network monitoring
- What is network management
- Getting started
- Why network management
- Attack detection
- Consolidating the data
- The big picture

What is network monitoring?

Anyone have some ideas?

Monitoring an active communications network in order to diagnose problems and gather statistics for administration and fine tuning.

WIKIPEDIA

*The term **network monitoring** describes the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator in case of outages via email, pager or other alarms. It is a subset of the functions involved in network management.*

What is network management?

(Webopedia)™

Refers to the broad subject of managing computer networks. There exists a wide variety of software and hardware products that help network system administrators manage a network. Network management covers a wide area, including:

- **Security:** Ensuring that the network is protected from unauthorized users.
- **Performance:** Eliminating bottlenecks in the network.
- **Reliability:** Making sure the network is available to users and responding to hardware and software malfunctions.

What is network management?

- **System & Service monitoring**
  - Reachability, availability
- **Resource measurement/monitoring**
  - Capacity planning, availability
- **Performance monitoring (RTT, throughput)**
- **Statistics & Accounting/Metering**
- **Fault Management (Intrusion Detection)**
  - Fault detection, troubleshooting, and tracking
  - Ticketing systems, help desk
- **Change management and configuration monitoring**

Getting started

Make sure that the network is up and running. Thus, we need to monitor it:

- Deliver projected SLAs (Service Level Agreements)
- Depends on policy
  - What does your management expect?
  - What do your users expect?
  - What do your customers expect?
  - What does the rest of the Internet expect?
- Is 24x7 good enough?
  - There's no such thing as 100% uptime (as we'll see) →

Getting started: “Uptime”

What does it take to deliver 99.9 % uptime?

30.5 x 24 = 762 hours a month

(762 – (762 x .999)) x 60 = 45 minutes

only 45 minutes of downtime a month!

Need to shutdown 1 hour / week?

(762 - 4) / 762 x 100 = 99.4 %

Remember to take planned maintenance into account in your calculations, and inform your users/customers if they are included/excluded in the SLA

How is availability measured?

In the core? End-to-end? From the Internet?

Getting started: Baselining

What is normal for your network?

If you've never measured or monitored your network you need to know things like:

- Load on links
- Jitter between endpoints
- Percent usage of resources
- Amount of "noise":
  - Network scans
  - Dropped data
  - Reported errors or failures

Why network management?

Know when to upgrade

- Is your bandwidth usage too high?
- Where is your traffic going?
- Do you need to get a faster line, or more providers?
- Is the equipment too old?

Keep an audit trace of changes

- Record all changes
- Makes it easier to find cause of problems due to upgrades and configuration changes

Keep a history of your network operations

- Using a ticket system let you keep a history of events.
- Allows you to defend yourself and verify what happened

Why network management?

Accounting

- Track usage of resources
- Bill customers according to usage

Know when you have problems

- Stay ahead of your users! Makes you look good.
- Monitoring software can generate tickets and automatically notify staff of issues.

Trends

- All of this information can be used to view trends across your network.
- This is part of baselining, capacity planning and attack detection.

Attack Detection

- Trends and automation allow you to know when you are under attack.
- The tools in use can help you to mitigate attacks:
  - Flows across network interfaces
  - Load on specific servers and/or services
  - Multiple service failures

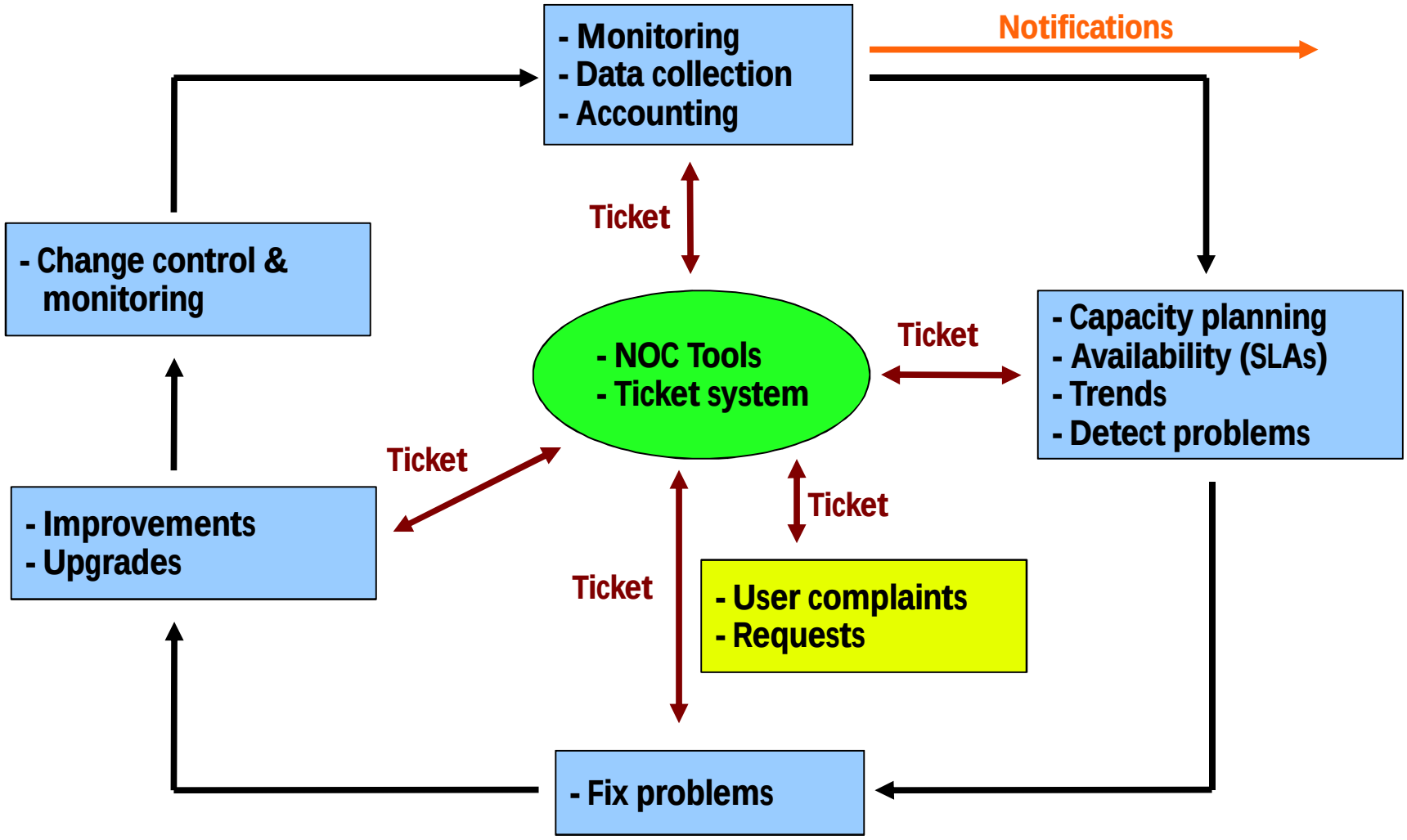
Consolidating the data

The Network Operations Center (NOC)

“Where it all happens”

- Coordination of tasks
- Status of network and services
- Fielding of network-related incidents and complaints
- Where the tools reside (”NOC server”)
- Documentation including:
  - Network diagrams
  - database/flat file of each port on each switch
  - Network description
  - Much more as you'll see a bit later.

The big picture



A *few* Open Source solutions…

Performance

- Cricket
- IFPFM
- flowc
- mrtg
- netflow
- NfSen
- ntop
- pmacct
- rrdtool
- SmokePing

SNMP/Perl/ping

- **Ticketing**
- RT, Trac, Redmine

Change Mgmt

- Mercurial
- Rancid (routers)
- RCS
- Subversion

Security/NIDS

- Nessus
- OSSEC
- Prelude
- Samhain
- SNORT
- Untangle

Net Management

- Big Brother
- Big Sister
- Cacti
- Hyperic
- Munin
- Nagios*
- Netdisco
- Netdot
- OpenNMS
- Sysmon
- Zabbix